UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,182	01/20/2004	John Brawner Duffie III	10-008	7709

23164 7590 02/23/2006

LEON R TURKEVICH
2000 M STREET NW
7TH FLOOR
WASHINGTON, DC 200363307

EXAMINER	
SERRAO, RANODHI N	
ART UNIT	**PAPER NUMBER**
2141	

DATE MAILED: 02/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/759,182	DUFFIE ET AL.	
	Examiner	Art Unit	
	Ranodhi Serrao	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Upon consideration of the applicant's response to the objection to the drawings, it is withdrawn.

2. Applicant's arguments filed on 04 January 2006 regarding the claims have been fully considered but they are not persuasive.

3. The applicant argued that Young et al. fails to teach the claimed features in independent claims 1, 10, 18, and 27 of controlling supply of data packets to a cryptographic module that generates encrypted packets for multiple secure connections. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., multiple secure connections) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Young teaches supporting encryption through software, see ¶ 98. This serves the function of controlling supply of data packets to a cryptographic module. As stated in the previous office action, "MAND serves the function of a cryptographic module." Secure connections or tunnels are disclosed as well in Young, see ¶ 97-98. Therefore Young teaches the invention as claimed.

4. Young also teaches priority queuing and routing, and configuring the bandwidths in ¶ 19. In ¶ 71-72 Young discloses a unique Transaction ID, this ID serves the purpose of a unique sequence number.

5. The examiner points out that the pending claims must be "given the broadest reasonable interpretation consistent with the specification" [In re Prater, 162 USPQ 541 (CCPA 1969)] and "consistent with the interpretation that those skilled in the art would reach" [In re Cortright, 49 USPQ2d 1464 (Fed. Cir. 1999)]. In conclusion, upon taking the broadest reasonable interpretation of the claims, the cited reference teaches all of the claimed limitations. And the rejections are reaffirmed. See below.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Young et al. (2003/0093563).

8. As per claim 1, Young et al. teaches a method in a router having at least one outbound interface (paragraph 0013), the method comprising: establishing, on the outbound interface, a plurality of Internet Protocol (IP-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module (paragraph 0098), each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number (paragraphs 0067 and 71-72); controlling supply of data packets to the cryptographic module (paragraph 0123: wherein MAND serves the function of a cryptographic module) by: (1) assigning, for each secure connection, a corresponding queuing module (paragraph 0051), (2) reordering, in each queuing module, a

corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy (paragraph 0009) and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module, and (3) outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets (paragraph 0051); and second outputting the encrypted packets from the cryptographic module to the one outbound interface for transport via their associated secure connections (paragraph 0098).

9. As per claim 10, Young et al. teaches a router comprising: a cryptographic module configured for successively outputting encrypted packets having respective successively-unique sequence numbers (paragraphs 0067 and 71-72); an outbound interface configured for establishing a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving respective streams of the encrypted packets (paragraph 0098); and a queue controller configured for controlling supply of data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module, each queuing module configured for: (I) outputting to the cryptographic module a corresponding group of the data packets associated with the corresponding secure connection (paragraph 0051), and according to a corresponding assigned maximum output bandwidth for the corresponding queuing module, for generation of the corresponding stream of the encrypted packets (paragraphs 0085-0087), and (2) reordering the corresponding group

of the data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth (paragraph 0009).

10. As per claim 18, Young et al. teaches a computer readable medium having stored thereon sequences of instructions for outputting encrypted packets by a router having at least one outbound interface, the sequences of instructions including instructions for: establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module (paragraph 0098), each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number (paragraphs 0067 and 71-72); controlling supply of data packets to the cryptographic module (paragraph 0123: wherein MAND serves the function of a cryptographic module) by: (1) assigning, for each secure connection, a corresponding queuing module (paragraph 0051), (2) reordering, in each queuing module, corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy (paragraph 0009) and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module (paragraph 0051), and (3) outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets (paragraph 0051); and second outputting the encrypted packets from the cryptographic module to the outbound interface for transport via their associated secure connections (paragraph 0098).

11. As per claim 27, Young et al. teaches A router having at least one outbound interface, the router further comprising: means for establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets (paragraph 0098); means for generating the encrypted packets, each encrypted packet successively output having a corresponding successively-unique sequence number (paragraphs 0067 and 71-72) and means for controlling supply of data packets to the generating means (paragraph 0123: wherein MAND serves the function of a cryptographic module), including: (1) means for assigning, for each secure connection, a corresponding queuing means for queuing data packets (paragraph 0051), (2) means for reordering, in each queuing means, a corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy (paragraph 0009) and based on a corresponding assigned maximum output bandwidth for the corresponding queuing means, the means for reordering configured for outputting to the generating means the group of data packets, from each corresponding queuing means according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets (paragraph 0098).

12. As per claims 2, 11, 19, and 28, Young et al. teaches a method, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface (paragraph 0009).

13. As per claims 3, 12, 20, and 29, Young et al. teaches a method, wherein the reordering step includes, in each queuing module: establishing a plurality of queues having respective identified priorities (paragraph 0051); storing each data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each data packet (paragraph 0019); and selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy (paragraph 0009).

14. As per claims 4, 21, and 30, Young et al. teaches a method, wherein: the establishing step includes establishing, on each of a plurality of the outbound interfaces (paragraph 0080), a corresponding plurality of the secure corrections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module (paragraph 0082); the controlling step includes controlling the supply of data packets, for each outbound interface, from the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections (paragraph 0150); the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router (paragraph 0098).

15. As per claims 5, 13, 22, and 31, Young et al. teaches a method, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol (paragraph 0123).

16. As per claims 6, 14, 23, and 32, Young et al. teaches a method, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream and an audio stream (paragraph 0053).

17. As per claims 7, 15, 24, and 33, Young et al. teaches a method, wherein the audio stream is a Voice over IP media stream (paragraph 0053).

18. As per claims 8, 16, 25, and 34, Young et al. teaches a method, wherein the controlling step further includes obtaining, for each queuing module, the corresponding assigned maximum output bandwidth from a configuration register (paragraph 0051).

19. As per claims 9, 17, 26, and 35, Young et al. teaches a method, wherein the controlling step further includes negotiating, for at least one queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination (paragraphs 0085-0087).

20. As per claim 21, Young et al. teaches a medium, wherein: the establishing step includes establishing, on each of a plurality of the outbound interfaces, a corresponding plurality of the secure connections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module (paragraph 0098); the controlling step includes controlling the supply of data packets, for each outbound interface, from the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections (paragraph 0150); the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing' decision executed by the router (paragraph 0098).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571)272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571)272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SUPERVISORY PATENT EXAMINER